Journal of Pure and Applied Algebra 66 (1990) 287–302
North-Holland

THE STRUCTURE OF SCHUR RINGS OVER CYCLIC GROUPS

Ka Hin LEUNG and Siu Lun MA

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 0511, Republic of Singapore

Communicated by A. Heller
Received 15 March 1989

Let G be a finite group and $D_1, D_2, \ldots, D_d$ be a partition of G. Suppose, for each $i = 1, 2, \ldots, d$, $\{g \in G \mid g^{-1} \in D_i\} = D_j$ for some j depending on i; and $\bar{D}_i \bar{D}_j = \sum_{h=1}^{d} p_{ij}^h \bar{D}_h$ for all $i, j = 1, 2, \ldots, d$ where $\bar{D}_m = \sum_{g \in D_m} g \in \mathbb{C}[G]$. Then the subalgebra of $\mathbb{C}[G]$ spanned by $\bar{D}_1, \bar{D}_2, \ldots, \bar{D}_d$ is called a Schur ring. Such an object is known to have application on group theory and combinatorial design theory. In this paper, we study the structure of Schur rings when G is a cyclic group. Two special cases are thoroughly determined. The first one concerns with the case that every D_i is fixed by Aut G. For the second one, we consider the case that G is a cyclic p-group. Also, examples of Schur rings with low dimension are given.

1. Introduction

Let G be a finite group. For any $B \subset G$ and $t \in \mathbb{Z}$, we define $\bar{B} = \sum_{g \in B} g \in \mathbb{C}[G]$ and $B^{(t)} = \{g^t \mid g \in B\}$. Also, if $x = \sum_{g \in G} a_g g \in \mathbb{C}[G]$ where $a_g \in \mathbb{C}$, then define $x^{(t)} = \sum_{g \in G} a_g g^t$. Let $D_1, D_2, \ldots, D_d$ be nonempty subsets of G with properties that

(I) $G = D_1 \cup D_2 \cup \cdots \cup D_d$ and $D_i \cap D_j = \emptyset$ if $i \neq j$;

(II) $D_i^{(-1)} = D_j$ for some j depending on i; and

(III) $\bar{D}_i \bar{D}_j = \sum_{h=1}^{d} p_{ij}^h \bar{D}_h$ for all i, j where p_{ij}^h are integers.

Then the subalgebra S of $\mathbb{C}[G]$ spanned by $\bar{D}_1, \bar{D}_2, \ldots, \bar{D}_d$ is called a *Schur ring* of dimension d over G. Each $\bar{D}_i$ is called a *principal basis element* of S and each D_i is called an *S-principal subset* of G. (In some literature, $\bar{D}_i$ is called a *simple basis element* of S and D_i is called an *S-class* of G.)

Remark. It is well known that S is a Schur ring over G if and only if S is a subalgebra of $\mathbb{C}[G]$ which is closed under the Hadamard product and $x^{(-1)} \in S$ for all $x \in S$. (The Hadamard product is the operation $\circ$ such that $(\sum_{g \in G} a_g g) \circ (\sum_{g \in G} b_g g) = \sum_{g \in G} a_g b_g g$ for any $\sum_{g \in G} a_g g$, $\sum_{g \in G} b_g g \in \mathbb{C}[G]$.)

A Schur ring S is called *unitary* if S contains the unit element e, where e is the identity element of G. In this case, $\{e\}$ is a S-principal subset of G. Also, S is called *symmetric* if $x^{(-1)} = x$ for all $x \in S$, i.e. $D^{(-1)} = D$ for every S-principal subset D.

Historically, Schur rings were first studied by Schur [10] and Wielandt [14] in their works concerning permutation groups. For applications of Schur rings on the group theory, please read [11], [13] and [15]. Recently it was found that Schur rings, especially those unitary and symmetric, were closely related to some combinatorial structures, e.g. association schemes and strongly regular graphs (see [1, 7]). Thus, the study of Schur rings becomes a topic in combinatorics as well as in group theory.

In the following, we prove some useful lemmas needed in latter sections. Note that S is always assumed to be a Schur ring over G. If ψ is a group homomorphism from G to H where H is a group, then we extend ψ to a homomorphism ψ^* from $\mathbb{C}[G]$ to $\mathbb{C}[H]$ such that $\psi^*(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \psi g$ where $a_g \in \mathbb{C}$. Also, for any $x, y, z \in \mathbb{C}[G]$, we say that $x \equiv y \bmod z$ if $x - y = wz$ for some $w \in \mathbb{C}[G]$.

Lemma 1.1. *Let H be a normal subgroup of G and $\varrho: G \to G/H$ be a natural epimorphism. Then there exists a Schur ring S' over G/H such that, for any $C \subset G/H$, $\bar{C} \in S'$ iff $\overline{\varrho^{-1}C} \in S$. Furthermore, if D is an S-principal subset of G and $\bar{D} \equiv 0 \bmod \bar{H}$, then ϱD is an S'-principal subset of G/H.*

Proof. Let $R = \{y \in S \mid y \equiv 0 \bmod \bar{H}\}$. Note that R is closed under addition, ordinary and Hadamard products. So it is a Schur subring of S. Thus $S' = \varrho^* R$ is the required Schur ring over G/H. □

Lemma 1.2. *Suppose there is a normal subgroup H of G such that $\bar{H} \in S$. Let $\varrho: G \to G/H$ be the natural epimorphism.*

(i) *If $D = g_1 A_1 \cup g_2 A_2 \cup \cdots \cup g_k A_k$ is an S-principal subset of G where A_i's are nonempty subsets of H and $g_1 H, g_2 H, \ldots, g_k H$ are distinct cosets of H, then $|A_1| = |A_2| = \cdots = |A_k|$.*

(ii) *If D_1, D_2 are S-principal subsets of G, then either $\varrho D_1 \cap \varrho D_2 = \emptyset$ or $\varrho D_1 = \varrho D_2$.*

(iii) *$\varrho^* S$ is a Schur ring over G/H. Furthermore, if D is a S-principal subset of G, then ϱD is a $\varrho^* S$-principal subset of G/H.*

Proof. For part (i), we have

$$\begin{aligned}\bar{D}\bar{H} &= |A_1| g_1 \bar{H} + |A_2| g_2 \bar{H} + \cdots + |A_k| g_k \bar{H} \\ &= \alpha \bar{D} + \sum \alpha_i \bar{D}_i\end{aligned}$$

for some integers α, α_i and S-principal subsets $D_i \neq D$. Obviously, $\alpha = |A_1| = |A_2| = \cdots = |A_k|$.

For part (ii), let $D_1 = g_1 B_1 \cup g_2 B_2 \cup \cdots \cup g_k B_k$ and $D_2 = g_1 C_1 \cup g_2 C_2 \cup \cdots \cup g_k C_k$ where $B_i, C_i \subset H$ and $g_1 H, g_2 H, \ldots, g_k H$ are distinct cosets of H. Assume that $\varrho D_1 \cap \varrho D_2 \neq \emptyset$, i.e. there is some j such that $B_j \neq \emptyset$ and $C_j \neq \emptyset$. As before, we see that

$$\bar{D}_1 \bar{H} = \alpha_1 \bar{D}_1 + \alpha_2 \bar{D}_2 + \cdots$$

for some positive integers α_1, α_2. Therefore, $B_i \neq \emptyset$ if $C_i \neq \emptyset$. Similarly, by considering $\bar{D}_2\bar{H}$, we get $C_i \neq \emptyset$ if $B_i \neq \emptyset$.

Finally, (iii) follows from (i) and (ii). □

Remark. In the latter sections, Lemmas 1.1 and 1.2 will be used as induction tools in the proof of some theorems and in the construction of Schur rings.

Lemma 1.3. *Let $D_1, D_2, \ldots, D_d$ be all the S-principal subsets of G. Suppose there is a $\sigma \in \mathrm{Aut}\, G$ such that $\sigma^* S = S$, i.e. σ permutes $D_1, D_2, \ldots, D_d$. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_b$ be orbits of σ acting on $D_1, D_2, \ldots, D_d$ and let $E_i = \bigcup_{D \in \mathcal{O}_i} D$, $i = 1, 2, \ldots, b$. Then $\bar{E}_1, \bar{E}_2, \ldots, \bar{E}_b$ spans a Schur subring of S.*

Proof. Let t be an integer such that $\sigma^t D_k = D_k$ for all k. For $1 \leq i, j \leq b$, $\bar{E}_i = (1/\alpha) \sum_{m=0}^{t-1} \sigma^{*m} \bar{D}_{i'}$ and $\bar{E}_j = (1/\beta) \sum_{m=0}^{t-1} \sigma^{*m} \bar{D}_{j'}$ for some $\bar{D}_{i'}$ and $\bar{D}_{j'}$. Let $\bar{D}_{i'}(\sigma^{*r} \bar{D}_{j'}) = \sum_{h=1}^{d} b_{ij}^{hr} \bar{D}_h$ for some integers b_{ij}^{hr}. Then

$$\bar{E}_i \bar{E}_j = \left[\frac{1}{\alpha} \sum_{m=0}^{t-1} \sigma^{*m} \bar{D}_{i'}\right]\left[\frac{1}{\beta} \sum_{m=0}^{t-1} \sigma^{*m} \bar{D}_{j'}\right]$$

$$= \frac{1}{\alpha\beta} \sum_{r=0}^{t-1} \sum_{s=0}^{t-1} \sigma^{*s}[\bar{D}_{i'}(\sigma^{*r} \bar{D}_{j'})]$$

$$= \frac{1}{\alpha\beta} \sum_{r=0}^{t-1} \sum_{h=1}^{d} b_{ij}^{hr} \left[\sum_{s=0}^{t-1} \sigma^{*s} \bar{D}_h\right]$$

which is clearly a linear combination of $\bar{E}_1, \bar{E}_2, \ldots, \bar{E}_b$. □

Remark. If G is abelian and $\sigma : g \mapsto g^t$ where t is relatively prime to $|G|$, then $\sigma \in \mathrm{Aut}\, G$ and $\sigma^* S = S$ (see [1, pp. 120–122]). Applying Lemma 1.3 repeatedly, one can obtain a Schur subring S_0 of S such that every S_0-principal subset is of the form $\bigcup_{(t,|G|)=1} D^{(t)}$ for some S-principal subset D. Such Schur rings will be studied in Section 2 for cyclic G.

Finally, we have a Lemma by Wielandt. A Schur ring S over G is called *primitive* if, for every S-principal subset D of G, the group $\langle D \rangle$ generated by D is either $\{e\}$ or G. Otherwise, it is called *imprimitive*. Note that if S is imprimitive and D is a S-principal subset of G such that $H = \langle D \rangle$ is a proper subgroup of G, then it can be shown that $\bar{H} \in S$ (see, for example, [1, Section 2.9]) and $S \cap \mathbb{C}[H]$ is a Schur ring over H.

Lemma 1.4 (Wielandt [15]). *If G is abelian and it contains a cyclic Sylow subgroup, then no primitive Schur ring of dimension $d > 2$ exists over G unless the order of G is a prime and, in this case, the principal subsets can be obtained as orbits of an automorphism of G.* □

Remark. The only primitive Schur ring of dimension 2 in any group G is the one spanned by $\bar{H}$ and $\bar{G}-\bar{H}$ where H is a subgroup of G.

2. Rational Schur rings over cyclic groups

In this section, we always assume G to be a cyclic group. Note that, in this case, $\sigma^*S=S$ for all $\sigma\in\mathrm{Aut}\,G$. We define that a Schur ring S is *rational* if $\sigma^*x=x$ for all $x\in S$ and all $\sigma\in\mathrm{Aut}\,G$ (see [7]). Otherwise, it is called *nonrational.*

For every $\sigma\in\mathrm{Aut}\,G$, there is an integer t relatively prime to $|G|$ such that $\sigma g=g^t$ for all $g\in G$. Thus, S is rational if and only if $D^{(t)}=D$ for all S-principal subsets D of G and all integers t relatively prime to $|G|$. This condition appears in the study of many combinatorial objects, e.g. partial difference sets, difference sets with -1 as multiplier and triple-sum-sets (see [2, 3, 5, 6]). Furthermore, by the remark below Lemma 1.3, it is known that any Schur ring S over G can be reduced to a rational Schur subring S_0 such that each S_0-principal subset is a union of S-principal subsets which are permuted by Aut G transitively. Thus, it is natural to ask how rational Schur rings look like.

In the following, we assume that S is a rational Schur ring over G.

Lemma 2.1. *Suppose $H\subsetneq G$ is a subgroup with $\bar{H}\in S$. Let p be a prime divisor of $|H|$ and P be the unique subgroup in H of order p. Then either*

(a) $\bar{D}\equiv 0 \bmod \bar{P}$ *for all S-principal subsets D contained in $G\setminus H$ or*

(b) *there exists a subgroup L of G such that $L\not\subset H$, $\bar{L}\in S$ and $p\nmid|L|$.*

Proof. Since G is cyclic, as noted in the proof of Lemma 1.4 by Wielandt [15, p. 65], we have $\bar{D}^{(p)}\equiv 0 \bmod p$ iff $\bar{D}\equiv 0 \bmod \bar{P}$. Assume that there is an S-principal subset $D\subset G\setminus H$ with $\bar{D}^{(p)}\not\equiv 0 \bmod p$. Let $\bar{D}^{(p)}=\sum_{g\in G} a_g g$ where a_g are nonnegative integers and $M=\{g\in G \mid p\nmid a_g\}$. For any $g\in M$, we claim that $p\nmid \mathrm{o}(g)$. If not, we let $T=\{h\in D \mid h^p=g\}\subset D$. It is clear that $p\mid \mathrm{o}(g)$ implies $p^2\mid \mathrm{o}(h)$ for all $h\in T$. As $D^{(t)}=D$ for all t relatively prime to $|G|$, we have $hP\subset D$. Hence $T=hP$ and $a_g=p$. This is a contradiction. Since $p\nmid \mathrm{o}(g)$ for all $g\in M$, it is obvious that $p\nmid|\langle M\rangle|$. Therefore, $L=\langle M\rangle$ satisfies (b). □

Theorem 2.2. *Suppose $H\subsetneq G$ is a subgroup with $\bar{H}\in S$. Then there exists another subgroup K of G such that $K\setminus H$ is an S-principal subset of G. Furthermore, if $D\subset HK\setminus(H\cup K)$ is an S-principal subset, then $D=E(K\setminus H)$ for some S-principal subset E contained in H.*

Proof. Firstly, let us show that there is a subgroup K of G such that $K\setminus H$ is an S-principal subset. If $H=\{e\}$, then it follows by Lemma 1.4. Assume it is true for all H with $|H|<m$. Now, let $|H|=m$, p be a prime divisor of m and P be the subgroup in H of order p. For case (a) of Lemma 2.1, we have $\bar{D}\equiv 0 \bmod \bar{P}$ for all

S-principal subsets D contained in $G \setminus H$. The subgroup K can be found by applying Lemma 1.1 and the inductive assumption. For case (b), there exists a subgroup L of G such that $p \nmid |L|$, $L \not\subset H$ and $\bar{L} \in S$. Let us consider the Schur ring $S \cap \mathbb{C}[L]$ over L. As $|L \cap H| \leq m/p$, by the inductive assumption, there exists a subgroup K of L such that $K \setminus H$ is an $(S \cap \mathbb{C}[L])$-principal subset of L. Certainly, $K \setminus H$ is an S-principal subset of G.

For the second part of the theorem, without loss of generality, we may assume $G = HK$. Let $D \subset G \setminus (H \cup K)$ be an S-principal subset. It is obvious that $D \subset E(K \setminus H)$ for some S-principal subset E contained in H.

If $H \cap K = \{e\}$, then $D = g_1 A_1 \cup g_2 A_2 \cup \cdots \cup g_k A_k$ where $A_i \subset E$ and $\{g_1, g_2, \ldots, g_k\} = K \setminus \{e\}$. Let q be a prime divisor of $|K|$. Note that $\bar{D}^{(q)} \equiv \bar{D}^q \bmod q$ and $\bar{D}^q$ is a linear combination of principal basis elements of S. Since $D^{(q)} \cap H \subset EK^{(q)} \cap H = E$, we have

$$\sum_{g_i^q \in H} \bar{A}_i = \sum_{g_i^q \in H} \bar{A}_i^{(q)} \equiv \alpha \bar{E} \bmod q$$

where α is an integer. However, $g_i^q \in H$ iff $g_i^q = e$ and there are exactly $q-1$ of them, say, $g_{i_0}, g_{i_0}^2, \ldots, g_{i_0}^{q-1}$. Since Aut G fixes D, we have $A_i = A_j$ whenever $g_i^t = g_j$ for some t relatively prime to $|G|$. Thus $(q-1)\bar{A}_{i_0} \equiv \alpha \bar{E} \bmod q$, i.e. $A_{i_0} = E$. By Lemma 1.2 and the fact that $K \setminus \{e\}$ is an S-principal subset, all A_i are nonempty and hence $|A_i| = |A_{i_0}| = |E|$ for all i. Since $A_i \subset E$, we get $A_i = E$. So $D = E(K \setminus \{e\})$.

Finally, let $H \cap K = N \neq \{e\}$. Let q' be a prime divisor of $|N|$ and Q be the subgroup in N of order q'. Note that if L is a subgroup in G with $q' \nmid |L|$ and $L \subset H$, then $L \cap (K \setminus N)$ is neither $K \setminus N$ nor $\emptyset$ and $\bar{L} \notin S$. With this observation and Lemma 2.1, we have $\bar{D} \equiv 0 \bmod \bar{Q}$. Applying Lemma 1.1 inductively, we find that $\bar{D} \equiv 0 \bmod \bar{N}$. Let $\varrho : G \to G/N$ be the natural epimorphism. By Lemma 1.2, ϱE, ϱD and $\varrho K \setminus \{e'\}$, where e' is the identity element in G/N, are $\varrho^* S$-principal subsets of G/N and $\overline{\varrho H} \in \varrho^* S$. Since $\varrho D \subset \varrho E(\varrho K \setminus \{e'\})$, $\varrho D \subset (G/N) \setminus (\varrho H \cup \varrho K)$ and $\varrho H \cap \varrho K = \{e'\}$, by previous argument, we get $\varrho D = \varrho E(\varrho K \setminus \{e'\})$. However $D = \varrho^{-1}[\varrho D] = \varrho^{-1}[\varrho E(\varrho K \setminus \{e'\})] = E(K \setminus N)$ because $\bar{D} \equiv \overline{K \setminus N} \equiv 0 \bmod \bar{N}$. □

Remark. Theorem 2.2 and Lemma 1.4 provide an inductive construction of all rational Schur rings over cyclic groups.

Corollary 2.3. *If S is a rational Schur ring over G, then there exists S-principal subsets $K_1 \setminus H_1, K_2 \setminus H_2, \ldots, K_t \setminus H_t$ where K_i, H_i are subgroups of G, such that every S-principal subset is product of some $K_i \setminus H_i$.*

Example. (See Fig. 1.) We list all rational Schur rings over cyclic groups with dimension $d \leq 5$. In the following, G is a cyclic group; $D_1, D_2, \ldots, D_d$ are all S-principal subsets and H, K, L, M are subgroups of G.

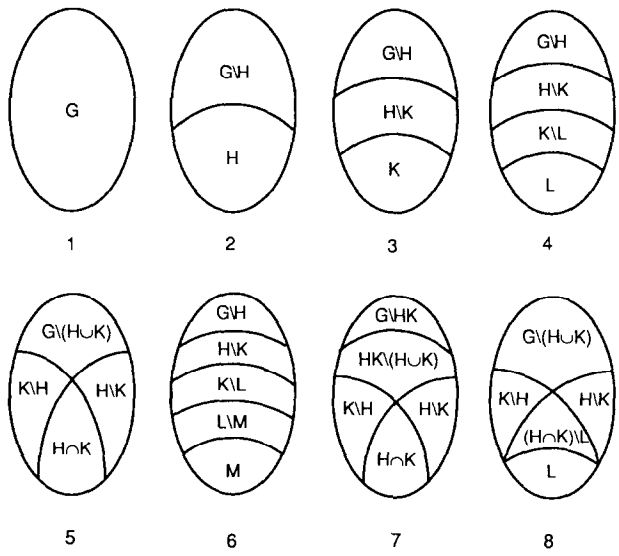

Fig. 1.

(1) $(d=1)D_1=G$.

(2) $(d=2)D_1=H$, $D_2=G\setminus H$ where $H\subsetneqq G$.

(3) $(d=3)D_1=K$, $D_2=H\setminus K$, $D_3=G\setminus H$ where $K\subsetneqq H\subsetneqq G$.

(4) $(d=4)D_1=L$, $D_2=K\setminus L$, $D_3=H\setminus K$, $D_4=G\setminus H$ where $L\subsetneqq K\subsetneqq H\subsetneqq G$.

(5) $(d=4)D_1=H\cap K$, $D_2=K\setminus H$, $D_3=H\setminus K$, $D_4=G\setminus(H\cup K)$ where $H\not\subset K$, $K\not\subset H$ and $HK=G$.

(6) $(d=5)D_1=M$, $D_2=L\setminus M$, $D_3=K\setminus L$, $D_4=H\setminus K$, $D_5=G\setminus H$ where $M\subsetneqq L\subsetneqq K\subsetneqq H\subsetneqq G$.

(7) $(d=5)D_1=H\cap K$, $D_2=K\setminus H$, $D_3=H\setminus K$, $D_4=HK\setminus(H\cup K)$, $D_5=G\setminus HK$ where $H\not\subset K$, $K\not\subset H$ and $HK\subsetneqq G$.

(8) $(d=5)D_1=L$, $D_2=(H\cap K)\setminus L$, $D_3=K\setminus H$, $D_4=H\setminus K$, $D_5=G\setminus(H\cup K)$ where $L\subsetneqq H\cap K$, $H\not\subset K$, $K\not\subset H$ and $HK=G$.

Remark. For the case of dimension $d=4$, i.e. Example 4 and 5, the result can be found in [8] with a tedious proof.

3. Cyclic p-groups

Let G be a cyclic group of order n. Let Ω be a subgroup of $\mathbb{Z}_n^*$. For $g\in G$, define $g^\Omega=\{g^t \mid t\in\Omega\}$. As Aut G is isomorphic to $\mathbb{Z}_n^*$, g^Ω can be regarded as the orbit of the corresponding automorphism group acting on g. Let D be an S-principal subset of G and $\Omega=\{t\in\mathbb{Z}_n^* \mid D^{(t)}=D\}$. Note that Ω is a subgroup of $\mathbb{Z}_n^*$. Moreover, there exist $g_1, g_2, \ldots, g_b$ in D such that $o(g_i)\neq o(g_j)$ whenever $i\neq j$ and $D=g_1^\Omega\cup g_2^\Omega\cup\cdots\cup g_b^\Omega$. Thus, in order to study the structure of Schur rings, we have to investigate g^Ω.

In this section, we shall concern us with cyclic p-groups only. Let G be a cyclic group of order p^s where p is a prime. For convenience, we denote the unique subgroup of order p^r by G_r. Also, we define $G_i=\{e\}$ if $i\leq 0$. In $\mathbb{Z}_{p^s}^*$, we define

$$\Lambda=\begin{cases}\{\alpha \mid \alpha\equiv 1 \bmod p\} & \text{if } p \text{ is odd,}\\ \{\alpha \mid \alpha\equiv 1 \bmod 4\} & \text{if } p=2.\end{cases}$$

It is well-known that Λ is a cyclic subgroup of $\mathbb{Z}_{p^s}^*$; $|\Lambda|=p^{s-1}$ if p is odd while $|\Lambda|=2^{s-2}$ if $p=2$; and

$$\mathbb{Z}_{p^s}^*=\begin{cases}I_{p-1}\times\Lambda & \text{if } p \text{ is odd where } I_{p-1} \text{ is the unique cyclic subgroup of order } p-1,\\ \langle -1\rangle\times\Lambda & \text{if } p=2.\end{cases}$$

For any subgroup Ω of $\mathbb{Z}_{p^s}^*$, we define $\Omega'=\Omega\cap\Lambda$. Obviously, $\Omega=\Omega'\cup t\Omega'\cup\cdots\cup t^{k-1}\Omega'$ for some $t\in\Omega$ and positive integer $k\leq p-1$. If p is odd, then t can be chosen in I_{p-1}. If $p=2$ and $\Omega\neq\Omega'$, then $t\equiv 3 \bmod 4$.

Lemma 3.1. *Let $g\in G_m\setminus G_{m-1}$ with $m\geq 1$ and Ω be a subgroup of $\mathbb{Z}_{p^s}^*$ with $|\Lambda/\Omega'|=p^a$.*

(i) *$g^{\Omega'}=gG_r$ where $r=m-a-1$ if p is odd and $r=m-a-2$ if $p=2$.*

(ii) *If Ω_1 is a subgroup of Ω, then g^{Ω} is a union of $(g^{t_i})^{\Omega_1}$ for some $t_i\in\Omega$.*

(iii) *If $\Omega\neq\Omega'$, then there exists $t\in\Omega$ and positive integer $k\leq p-1$ such that $g^{\Omega}=gG_r\cup g^tG_r\cup\cdots\cup g^{t^{k-1}}G_r$ where t can be chosen in I_{p-1} when p is odd and $t\equiv 3 \bmod 4$ when $p=2$. Moreover, $g^{t^i}G_{m-1}\neq gG_{m-1}$ for $1\leq i\leq k-1$ if p is odd; and $g^tG_{m-2}\neq gG_{m-2}$ if $p=2$ and $m\geq 2$.*

Proof. $|\Omega'|=p^{s-j}$ where $j=a-1$ if p is odd and $j=a-2$ if $p=2$. Obviously, $\{\alpha\in\mathbb{Z}_{p^s}^* \mid \alpha\equiv 1 \bmod p^j\}$ is a multiplicative group of order p^{s-j} and hence is equal to Ω'. Thus $g^{\Omega'}=gH$ where $H=\langle g^{p^j}\rangle$. As $o(g^{p^j})=\max\{p^{m-j},1\}$, (i) follows. (ii) is obvious. For (iii), the first part follows from the fact that $\Omega=\Omega'\cup t\Omega'\cup\cdots\cup t^{k-1}\Omega'$. When p is odd, $t^i\not\equiv 1 \bmod p$ for $1\leq i\leq k-1$ and therefore $g^{t^i}G_{m-1}\neq gG_{m-1}$. Similarly, $g^tG_{m-2}\neq gG_{m-2}$ when $p=2$. □

Let Ω be any subgroup in $\mathbb{Z}_{p^s}^*$. Suppose $|\Lambda/\Omega'|=p^a$. We define

$$\Omega[-i]=\begin{cases}\Omega\,\Omega[-i]' & \text{if } 1\leq i\leq a,\\ \mathbb{Z}_{p^s}^* & \text{if } i>a,\end{cases}$$

where $\Omega[-i]'$ is the unique subgroup in Λ of order $p^i|\Omega'|$. Following the notation of Lemma 3.1, we illustrate the significance of defining $\Omega[-i]$. Taking any $h\in G_w\setminus G_{w-1}$ where $r<w<m$, we have

$$hG_r\cup h^tG_r\cup\cdots\cup h^{t^{k-1}}G_r=h^{\Omega[-(m-w)]}.$$

Lemma 3.2. *If $h\in G_m$, then*

$$\overline{g^{\Omega}}(h+h^t+\cdots+h^{t^{k-1}})$$

$$=\begin{cases}\sum \overline{g_i^{\Omega}} & \text{if } h\in G_{m-1},\\ \alpha\sum \overline{g_i^{\Omega}}+\beta\overline{h_1^{\Omega[-(m-j)]}} \text{ or } \alpha\sum \overline{g_i^{\Omega}}+\beta\bar{G}_r & \text{if } h\in G_m\setminus G_{m-1} \text{ and } p \text{ is odd},\\ \alpha\overline{h_0^{\Omega[-1]}}+\beta\overline{h^{\Omega[-(m-j)]}} \text{ or } \alpha\overline{h_0^{\Omega[-1]}}+\beta\bar{G}_r & \text{if } h\in G_m\setminus G_{m-1} \text{ and } p=2,\end{cases}$$

where α, β *are nonnegative integers,* $g_i\in G_m\setminus G_{m-1}$, $h_0\in G_{m-1}\setminus G_{m-2}$ *and* $h_1\in G_j\setminus G_{j-1}$ *for* $r<j<m$.

Proof. When p is odd, as $t\in I_{p-1}$, the multiplication can be reduced to the addition of cyclotomic classes (see [12]). For $p=2$, $g^{\Omega}=gG_r$ or $gG_r\cup g^tG_r$. The lemma can be shown by direct computation. □

Let S be a Schur ring over a cyclic p-group G. As discussed in the remark following Lemma 1.3, we can construct a Schur subring S_o such that every S_o-principal subset is of the form $\bigcup_{t\uparrow p} D^{(t)}$ for some S-principal subset D. Clearly, S_o is rational. Therefore, it follows from the results in Section 2 that there exists a chain of subgroups

$$H_1\subsetneqq H_2\subsetneqq\cdots\subsetneqq H_w=G$$

such that $H_1, H_2\setminus H_1, \ldots, H_w\setminus H_{w-1}$ are all the S_o-principal subsets. For convenience, we set $H_0=\emptyset$. Suppose $D_i\subset H_i\setminus H_{i-1}$ is an S-principal subset. Let $\Omega_i=\{t\in\mathbb{Z}_{p^s}^*\mid D_i^{(t)}=D_i\}$. By the construction of $H_i\setminus H_{i-1}$, we see that every S-principal subset in $H_i\setminus H_{i-1}$ is of the form $D_i^{(t)}$ for some $t\in\mathbb{Z}_{p^s}^*$. It follows that $H_i\setminus H_{i-1}=\bigcup_{t\uparrow p} D_i^{(t)}$ and that Ω_i fixes every S-principal subset in $H_i\setminus H_{i-1}$. In other words, Ω_i does not depend on the choice of S-principal subset in $H_i\setminus H_{i-1}$. Thus we obtain subgroups $\Omega_1,\Omega_2,\ldots,\Omega_w$ of $\mathbb{Z}_{p^s}^*$ associated with S. These subgroups turn out to be crucial in determining the structure of S and they are closely related as we shall see. From now on, we shall use the notations defined above unless otherwise stated.

Theorem 3.3. $H_i\setminus H_{i-1}$ *is an* S*-principal subset iff* $\Omega_i=\mathbb{Z}_{p^s}^*$. *Moreover if* $|H_i/H_{i-1}|>p$, *then* $H_i\setminus H_{i-1}$ *is an* S*-principal subset.*

Proof. The first statement is clear from the above discussion. For the second statement, without loss of generality, we may assume $G=H_i$. For convenience, we denote H_{i-1} by H and Ω_i by Ω. Let D be an S-principal subset in $G\setminus H$. As $G\setminus H=\bigcup_{t\uparrow p} D^{(t)}$, there exists a generator g of G in D. Let $m=|G/H|$. By assumption, we have $m>p$.

Clearly, $D=\bigcup_{j=1}^{m-1} g^jA_j$ for some $A_j\subset H$. If $A_j=\emptyset$ for some j, then, by Lemma 1.2(iii), we can obtain a primitive Schur ring over G/H of dimension $d>2$. Hence, by Lemma 1.4, $|G/H|=p$. This is a contradiction.

Now assume $A_j \neq \emptyset$ for all j. As discussed in the beginning of this section, the set of generators of G contained in D is g^{Ω}. By Lemma 3.1(iii), we see that $g^{p+1}A_{p+1} \subset g^{\Omega'} = gG_{s-1} \cap D$ when p is odd; $g^5 A_5 \subset g^{\Omega'} = gG_{s-2} \cap D$ when $p=2$ and $m>4$. We first consider the case when p is odd. Obviously, for any $h \in A_{p+1}$, $o(g^p h) = p^{s-1}$. Therefore $|\Omega'| = p^{s-1}$ and hence $gH \subset D$ by Lemma 3.1(i). It follows from Lemma 1.2(i) that all $A_j = H$ and $D = G \setminus H$. In case of $p=2$ and $m>4$, we get similar result.

The remaining case is $p=2$ and $m=4$. By Lemma 3.1(iii), we can write $D = gG_r \cup g^t G_r \cup g^2 A$ where $A \subset H$ and $t \in \Omega$ with $t \equiv 3 \bmod 4$. If $r=0$, then by Lemma 1.2(i), $|A| = 1$, say $g^2 A = g^{2\alpha}$ for some odd α. Since $D^{(t)} = D$, we have $g^{2t} = g^2$, i.e. $t \equiv 1 \bmod 2^{s-1}$. However, this means $|G| = 4$ and $D = G \setminus H$. On the other hand, if $r = s-2$, then it is not possible by Lemma 1.2(i). Therefore, we may assume $1 \leq r \leq s-3$. In this case, $g^2 A = g^{2\alpha} G_{r-1} \cup g^{2\alpha t} G_{r-1}$ for some odd t. As $r \leq s-3$, we have $g^{2\alpha} G_r \neq g^{2\alpha t} G_r$ by Lemma 3.1(iii). Also, observe that $\bar{D}^2 \equiv |G_{r-1}|(g^{4\alpha}\bar{G}_{r-1} + g^{4\alpha t}\bar{G}_{r-1}) \not\equiv 0 \bmod |G_r|$ as $g^{4t} \notin G_r$. Hence $g^{4\alpha}\bar{G}_{r-1} + g^{4\alpha t}\bar{G}_{r-1} \in S$. Note that $g^{2^i\alpha}\bar{G}_{r-1} + g^{2^i \alpha t}\bar{G}_{r-1} \in S$ implies $g^{2^{i+1}\alpha}\bar{G}_{r-1} + g^{2^{i+1}\alpha t}\bar{G}_{r-1} \in S$. Therefore, by induction, we get

$$\overline{G_{r+1} \setminus G_r} = g^{2^{s-r+1}\alpha}\bar{G}_{r-1} + g^{2^{s-r+1}\alpha t}\bar{G}_{r-1} \in S.$$

Hence $\bar{G}_r \in S$. By Lemma 1.2(i), $g^{2\alpha} G_r \subset D$. Therefore, $g^{2\alpha} G_{r-1} \cup g^{2\alpha t} G_{r-1} = g^{2\alpha} G_r$ and this implies $g^{2\alpha} G_r = g^{2\alpha t} G_r$. This is a contradiction. □

Theorem 3.4. *Suppose $H_i \setminus H_{i-1} = G_m \setminus G_{m-1}$ is not an S-principal subset, i.e. $\Omega_i \neq \mathbb{Z}_{p^s}^*$, and $|A/\Omega_i'| = p^a$. Then there exist $t \in \Omega_i$ (if p is odd, $t \in \Omega_i \cap I_{p-1}$) and $k \in \mathbb{N}$ such that any S-principal subset in $G_m \setminus G_{m-1}$ is of the form*

$$g^{\Omega_i} = gG_r \cup g^t G_r \cup \cdots \cup g^{t^{k-1}} G_r$$

for some $g \in G_m \setminus G_{m-1}$, where $r = m-a-1$ when p is odd and $r = m-a-2$ when $p=2$. Furthermore, for $1 \leq j \leq a$, we have

(i) $H_{i-j} \setminus H_{i-j-1} = G_{m-j} \setminus G_{m-j-1}$;

(ii) $\Omega_{i-j} \subset \Omega_i[-j]$;

(iii) $|\Omega_{i-j}/\Omega_{i-j}'| = |\Omega_i/\Omega_i'|$ *and*

(iv) $\overline{G_{r+1} \setminus G_r} \in S$ *when* $p=2$.

Proof. The fact that every S-principal subset in $H_i \setminus H_{i-1}$ is of the form g^{Ω_i} for some $g \in G_m \setminus G_{m-1}$ follows from the definition of Ω_i and Theorem 3.3. Also, the expression of g^{Ω_i} in term of G_r follows from Lemma 3.1(iii).

Note that we have nothing to prove for (i), (ii) and (iii) when $a=0$. For $p=2$ and $a=0$, as $\Omega_i \neq \mathbb{Z}_{p^s}^*$, $\Omega_i = A$. So $g^{\Omega_i} = gG_{m-2}$ and hence $g^2 \bar{G}_{m-2} = \overline{G_{m-1} \setminus G_{m-2}} \in S$. Thus, we may assume $a \geq 1$ and $r \leq m-2$ when p is odd; $r \leq m-3$ when $p=2$. Observe that

$$(\overline{g^{\Omega_i}})^p \equiv |G_r|^{p-1}(g^p + g^{pt} + \cdots + g^{pt^{k-1}})\bar{G}_r \mod p|G_r|^{p-1}$$

and that by Lemma 3.1(iii), $g^{pt^i}G_r \neq g^{pt^j}G_r$ for $i \not\equiv j \bmod k$. Hence

$$\overline{(g^p)^{\Omega_i[-1]}} = g^p G_r + g^{pt} G_r + \cdots + g^{pt^{k-1}} G_r \not\equiv 0 \mod p$$

and it is an element in S. It follows that $H_{i-1} \setminus H_{i-2} = G_{m-1} \setminus G_{m-2}$ and $\Omega_{i-1} \subset \Omega_i[-1]$.

Firstly, we shall deal with the case when p is odd. In this case, $t \in I_{p-1}$. Hence $\Omega_{i-1} = \Omega'_{i-1} \cup t^c \Omega'_{i-1} \cup \cdots \cup t^{c(b-1)} \Omega'_{i-1}$ for some c and b where $0 \leq c \leq k-1$, $1 \leq b \leq k$ and $cb \equiv 0 \bmod k$. So there exists a subgroup H of G_r such that, for any $h \in G_{m-1} \setminus G_{m-2}$,

$$h^{\Omega_{i-1}} = hH \cup h^{tc} H \cup \cdots \cup h^{tc(b-1)} H$$

is an S-principal subset in $H_{i-1} \setminus H_{i-2}$. Multiplying $\overline{g^{\Omega_i}}$ with $\overline{h^{\Omega_i[-1]}}$, we get

$$\overline{g^{\Omega_i}}\,\overline{h^{\Omega_i[-1]}} = |H| \sum_{\varepsilon=1}^{k-1} \sum_{\delta=1}^{b-1} g^{t^\varepsilon} h^{t^{c\delta}} \bar{G}_r = \sum \overline{g_j^{\Omega_i}}$$

for some $g_j \in G_m \setminus G_{m-1}$. As $gh\bar{G}_r$ appears in the middle term, $g^t h^t \bar{G}_r$ also appears. Thus $g^t h^t \bar{G}_r = g^{t^\varepsilon} h^{t^{c\delta}} \bar{G}_r$ for some ε and δ. Applying Lemma 3.1(iii) twice, we see that $\varepsilon = 1$, $\delta = 1$ and $c = 1$. It follows that $\Omega_{i-1} = \langle t \rangle \Omega'_{i-1}$.

For $p = 2$, if $k = 1$ (i.e. $\Omega_i \subset \Lambda$), then clearly $\Omega_{i-1} \subset \Lambda$ and so $|\Omega_{i-j}/\Omega'_{i-j}| = |\Omega_i/\Omega'_i| = 1$; if $k = 2$ (i.e. $\Omega_i \subset \Lambda$), then by the fact that $g^t h G_r \neq g^t h^t G_r$, we see that $\Omega_{i-1} \subset \Lambda$ and we have $|\Omega_{i-j}/\Omega'_{i-j}| = |\Omega_i/\Omega'_i| = 2$.

Using the arguments above, for both even and odd p, we can prove (i), (ii) and (iii) inductively.

For (iv), we observe that $H_{i-a+1} \setminus H_{i-1} = G_{r+3} \setminus G_{r+2}$ and that $\Omega_{i-a+1} \neq \mathbb{Z}_{2^s}^*$. By (i), (iv) is obvious if $|\Lambda/\Omega'_{i-a+1}| \geq 4$. So we may assume $|\Lambda/\Omega'_{i-a+1}| = 2$. Every S-principal subset in $G_{r+3} \setminus G_{r+2}$ is of the form hG_r or $hG_r \cup h^t G_r$ for some $h \in G_{r+3}$ and $t \in \Omega_{i-a+1} \setminus \Lambda$. For the former case, $h^4 \bar{G}_r = \overline{G_{r+1} \setminus G_r} \in S$. For the latter case,

$$(h\bar{G}_r + h^t \bar{G}_r)^2 = h^2 \bar{G}_r + h^{2t} \bar{G}_r + 2hh^t \bar{G}_r.$$

It follows that $hh^t \bar{G}_r \in S$ as $h^2 \bar{G}_r + h^{2t} \bar{G}_r \in S$. It is clear that $hh^t G_r = G_r$ or $G_{r+1} \setminus G_r$. In both cases, we have $\overline{G_{r+1} \setminus G_r} \in S$. □

Corollary 3.5. *Let the notation be as in Theorem* 3.4. *Suppose D is an S-principal subset in H_{i-1}. Then*

$$\bar{D}\bar{G}_r = \begin{cases} |D|\,\bar{G}_r & \text{if } D \subset G_r, \\ \dfrac{|D|}{k}(h + h^t + \cdots + h^{t^{k-1}})\bar{G}_r & \text{if } D \subset H_{i-1} \setminus G_r \quad \text{where } h \in D. \end{cases}$$

Proof. Certainly, the corollary is true if $D \subset G_r$ or if $p = 2$ and $D \subset G_{r+1} \setminus G_r$. Otherwise, let $D \subset H_{i-j} \setminus H_{i-j-1}$ for some $j \geq 1$, then, by Theorem 3.4, $D = hK \cup h^{t'} K \cup \cdots \cup h^{t'^{k-1}} K$ where $h \in D$, $t' \in \Omega_{i-j} \setminus \Omega_{i-j-1}$ and K is a subgroup of

G_r. Hence $\bar{D}\bar{G} = |K|(h + h^{t'} + \cdots + h^{t'^{k-1}})\bar{G}_r$. If p is odd, then we can choose $t' = t \in I_{p-1}$. For $p = 2$, if $k = 1$, it is obvious; and if $k = 2$, then

$$(h + h^t)\bar{G}_r = \overline{g^{\Omega_{i-j}[-j]}} = (h + h^{t'})\bar{G}_r. \qquad \square$$

We can now describe inductively the structure of all Schur rings over any cyclic p-group. Let G be a cyclic group of order p^s and $G_m \subsetneqq G$. Our goal is to construct a Schur ring S such that G_m is the largest subgroup with $\overline{G \setminus G_m} \in S$. Let S' be a Schur ring over G_m. Clearly, $S' \cup \{\overline{G \setminus G_m}\}$ spans a Schur ring over G satisfying our requirements. In fact, by Theorem 3.3, this is the only possible case if $m < s-1$. Let us now assume $m = s-1$. There exists a chain of subgroups

$$K_1 \subsetneqq K_2 \subsetneqq \cdots \subsetneqq K_v = G_{s-1}$$

such that for any S'-principal subset D in $K_i \setminus K_{i-1}$, then $K_i \setminus K_{i-1} = \bigcup_{t \in I_p} D^{(t)}$. Let Ω_i be the subgroup in $\mathbb{Z}_{p^s}^*$ which fixes all S'-principal subsets in $K_i \setminus K_{i-1}$. By Theorem 3.4, Corollary 3.5 and Lemma 3.2, we have the following result:

Theorem 3.6. *Let Ω be a subgroup in $\mathbb{Z}_{p^s}^*$ and let S be a subalgebra of $\mathbb{C}[G]$ spanned by $S' \cup \{\overline{g^{\Omega}} \mid g \in G \setminus G_{s-1}\}$. Then S is a Schur ring over G if and only if one of the following conditions is satisfied:*

(i) *p is odd and $\Omega \supset \Lambda$.*

(ii) *p is odd, $\Omega[-1] \supset \Omega_v$ and $|\Omega/\Omega'| = |\Omega_v/\Omega_v'|$.*

(iii) *$p = 2$ and $\Omega = \mathbb{Z}_{2^s}^*$*

(iv) *$p = 2$, $\Omega = \Lambda$ and $K_v \setminus K_{v-1} = G_{s-1} \setminus G_{s-2}$.*

(v) *$p = 2$, $\Omega[-1] \supset \Omega_v$, $|\Omega/\Omega'| = |\Omega_v/\Omega_v'|$, $K_v \setminus K_{v-1} = G_{s-1} \setminus G_{s-2}$ and $K_{v-1} \setminus K_{v-2} = G_{s-2} \setminus G_{s-3}$.*

Remark. For (v), the condition $|\Omega/\Omega'| = |\Omega_v/\Omega_v'|$ would imply $K_v \setminus K_{v-1} = G_{s-1} \setminus G_{s-2}$ and $K_{v-1} \setminus K_{v-2} = G_{s-2} \setminus G_{s-3}$, if $\Omega_v \neq \mathbb{Z}_{p^s}^*$.

Example. (See Fig. 2.) In the following, we shall list all nonrational Schur rings over cyclic p-groups G with dimension $d \leq 5$ (the rational cases are given as Examples 1, 2, 3, 4, 6 in Section 2). For convenience, we shall denote all the S-principal subsets by $D_1, D_2, \ldots, D_d$. Whenever L, K, H are used, we assume that they are subgroups of G and

$$L \subsetneqq K = \langle k \rangle \subsetneqq H = \langle h \rangle \subsetneqq G = \langle g \rangle.$$

If p is odd, we let t be a generator of $\mathbb{Z}_{p^s}^*$ and $\Delta_m \subset \mathbb{Z}_{p^s}^*$ be a subgroup of index $m \mid p-1$.

(1) $(d=3)$ $D_1 = H$, $D_2 = g^{\Delta_2}H$, $D_3 = g^{t\Delta_2}H$ where p is odd and $[G:H] = p$.

(2) $(d=4)$ $D_1 = K$, $D_2 = h^{\Delta_2}K$, $D_3 = h^{t\Delta_2}K$, $D_4 = G \setminus H$ where p is odd and $[H:K] = p$.

(3) $(d=4)$ $D_1 = K$, $D_2 = H \setminus K$, $D_3 g^{\Delta_2}H$, $D_4 = g^{t\Delta_2}H$ where p is odd and $[G:H] = p$.

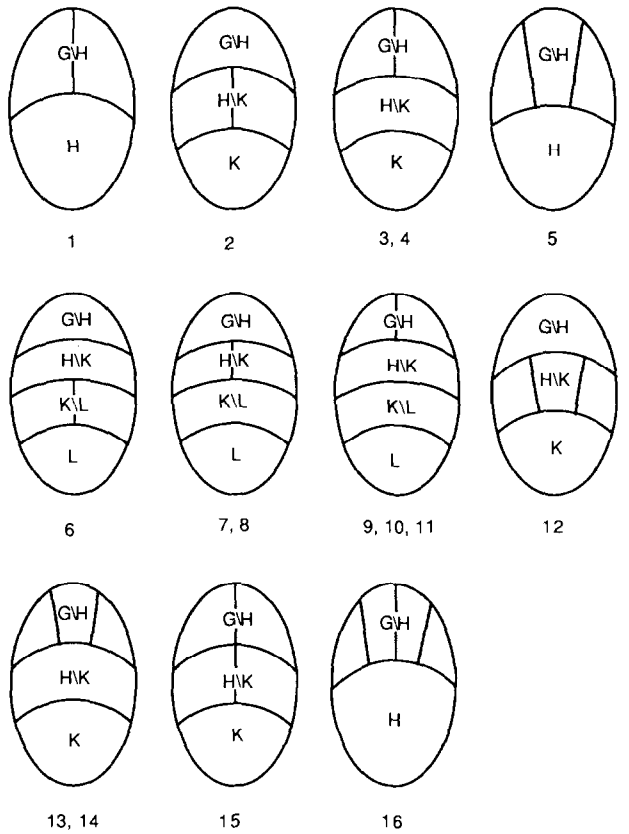

Fig. 2.

(4) $(d=4)D_1=K$, $D_2=g^2K$, $D_3=gK$, $D_4=g^3K$ where $p=2$ and $[G:K]=4$.

(5) $(d=4)D_1=H$, $D_2=g^{\Delta_3}H$, $D_3=g^{t\Delta_3}H$, $D_4=g^{t^2\Delta_3}H$ where $p\equiv 1 \bmod 3$ and $[G:H]=p$.

(6) $(d=5)D_1=L$, $D_2=k^{\Delta_2}L$, $D_3=k^{t\Delta_2}L$, $D_4=H\setminus K$, $D_5=G\setminus H$ where p is odd and $[K:L]=p$.

(7) $(d=5)D_1=L$, $D_2=K\setminus L$, $D_3=h^{\Delta_2}K$, $D_4=h^{t\Delta_2}K$, $D_5=G\setminus H$ where p is odd and $[H:K]=p$.

(8) $(d=5)D_1=L$, $D_2=h^2L$, $D_3=hL$, $D_4=h^3L$, $D_5=G\setminus H$ where $p=2$ and $[G:L]=4$.

(9) $(d=5)D_1=L$, $D_2=K\setminus L$, $D_3=H\setminus K$, $D_4=g^{\Delta_2}H$, $D_5=g^{t\Delta_2}H$ where p is odd and $[G:H]=p$.

(10) $(d=5)D_1=L$, $D_2=K\setminus L$, $D_3=g^2K$, $D_4=gK$, $D_5=g^3K$ where $p=2$ and $[G:K]=4$.

(11) $(d=5)D_1=L$, $D_2=g^4L$, $D_3=g^2L\cup g^6L$, $D_4=gL\cup g^{\alpha}L$, $D_5=g^5L\cup g^{5\alpha}L$ where $p=2$, $[G:L]=8$ and $\alpha=3$ or 7.

(12) $(d=5)D_1=K$, $D_2=h^{\Delta_3}K$, $D_3=h^{t\Delta_3}K$, $D_4=h^{t^2\Delta_3}K$, $D_5=G\setminus K$ where $p\equiv 1 \bmod 3$ and $[H:K]=p$.

(13) $(d=5)D_1=K$, $D_2=H\setminus K$, $D_3=g^{\Delta_3}K$, $D_4=g^{t\Delta_3}K$, $D_5=g^{t^2\Delta_3}K$ where $p\equiv 1 \bmod 3$ and $[G:H]=p$.

(14) $(d=5)D_1=H$, $D_2=g^3K\cup g^6K$, $D_3=gK\cup g^{-1}K$, $D_4=g^4K\cup g^{-4}K$, $D_5=g^7K\cup g^{-7}K$ where $p=3$ and $[G:K]=9$.

(15) $(d=5)D_1=K$, $D_2=h^{\Delta_2}K$, $D_3=h^{t\Delta_2}K$, $D_4=g^{\Delta_2}H$, $D_5=g^{t\Delta_2}H$ where p is odd and $[G:H]=[H:K]=p$.

(16) $(d=5)D_1=H$, $D_2=g^{\Delta_4}H$, $D_3=g^{t\Delta_4}H$, $D_4=g^{t\Delta_4}H$, $D_5=g^{t^3\Delta_4}H$ where $p\equiv 1 \bmod 4$ and $[G:H]=p$.

4. Cyclic Schur rings of low dimension

In this section, we study cyclic Schur rings of dimension d when d is small. For $d=1$ and 2, the Schur rings must be rational and hence are given as Examples 1 and 2 in Section 2. Now, we study the case when $d=3$ or 4.

Let G be a cyclic group of order n and S be a Schur ring over G. Suppose D is an S-principal subset of G and $\Omega=\{t\in\mathbb{Z}_n^* \mid D^{(t)}=D\}$. As we have seen before, Ω is a subgroup of $\mathbb{Z}_n^*$. If $|\mathbb{Z}_n^*/\Omega|=m$, then there are exactly m distinct $D^{(t)}$'s for t relatively prime to n. Also, there exists $g_1, g_2, \ldots, g_b$ in D such that $o(g_i)\neq o(g_j)$ whenever $i\neq j$ and $D=g_1^{\Omega}\cup g_2^{\Omega}\cup\cdots\cup g_b^{\Omega}$. Obviously, $|g_i^{\Omega}|=\varphi(o(g_i))/m$ for all i where φ is the Euler function.

Theorem 4.1. *Let H be a subgroup of G with $\bar{H}\in S$ and D be an S-principal subset contained in $G\setminus H$. Suppose $D\neq G\setminus H$ and $\bigcup_{(t,|G|)=1} D^{(t)}=G\setminus H$. Then the index of H over G is a prime p and $\bar{D}\equiv 0 \bmod H_0$ where H_0 is the subgroup of H containing all elements of order not divisible by p.*

Proof. In the discussion above, we see that $\Omega=\{t\in\mathbb{Z}_n^* \mid D^{(t)}=D\}$ is a subgroup in $\mathbb{Z}_n^*$. For $k\mid n$, define $\Omega(k)=\{t'\in\mathbb{Z}_k^* \mid t'\equiv t \bmod k \text{ for some } t\in\Omega\}$ which is a projection of Ω on $\mathbb{Z}_k^*$. If there exists $g\in D$ with $o(g)=k$, then $g^{\Omega}=g^{\Omega(k)}$. In this case, $|\Omega(k)|=|g^{\Omega(k)}|=\varphi(k)/m$ where $m=|\mathbb{Z}_n^*/\Omega|$.

Let p be a prime divisor of $|G/H|$ and $p^s \| |G|$. Suppose there is another prime divisor q of $|G/H|$ and $q^t \| |G|$. Then there are elements $g_1, g_2, g_3\in D$ with $o(g_1)=p^s$, $o(g_2)=q^t$ and $o(g_3)=p^sq^t$. Hence

$$|\Omega(p^s)|=\frac{\varphi(p^s)}{m}, \quad |\Omega(q^t)|=\frac{\varphi(q^t)}{m} \quad \text{and} \quad |\Omega(p^sq^t)|=\frac{\varphi(p^sq^t)}{m}.$$

But by the Chinese Remainder Theorem, we have $|\Omega(p^sq^t)|\leq|\Omega(p^s)|\ |\Omega(q^t)|$. Thus $m=1$ and $D=G\setminus H$. So if $D\neq G\setminus H$, then $|G/H|$ is a power of p.

Now, let π be a prime divisor of $|H|$ and $\pi\neq p$. Suppose $p^r \| |H|$. Since the order of every element in D is divisible by p^{r+1}, the order of every element in $D^{(\pi)}$ is divisible by p^{r+1}. So, we conclude $D^{(\pi)}\subset G\setminus H$. However, $D^{(\pi)}$ does not contain any generators of G. $\bar{D}^{(\pi)}$ must not be a linear combination of $\bar{D}^{(t)}$'s. Thus $\bar{D}^{(\pi)}\equiv 0$

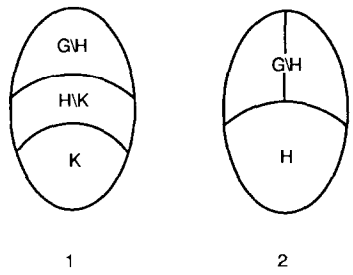

Fig. 3.

mod π. It follows that $\bar{D} \equiv 0 \bmod \bar{\Pi}$ where Π is a subgroup in H of order π. Applying Lemma 1.1 inductively, we have $\bar{D} \equiv 0 \bmod \bar{H}_0$ and we reduce G to a group of order p^s. The theorem follows by applying Theorem 3.3. □

Remark. Since $\bar{D} \equiv 0 \bmod \bar{H}_0$, by considering the projection of S onto $\mathbb{C}[G/H_0]$, we obtain some necessary conditions on the structure of S by Theorem 3.4. By decomposing rational Schur rings of dimension $d=2$ and 3 under these conditions, we obtain all nonrational Schur rings of dimension $d-3$ and 4.

In the following, G is a cyclic group, $D_1, D_2, \ldots, D_d$ are all the S-principal subsets, H, K, L are subgroups of G and p is a prime. If $[G:H]=p$, let $g \in G \setminus H$ be such that the order of g is a power of p; and if $[H:K]=p$, let $h \in H \setminus K$ be such that the order of h is a power of p. If p is odd and $p^s \| |G|$, we let t be a generator of $\mathbb{Z}_{p^s}^*$ and $\Delta_m \subset \mathbb{Z}_{p^s}^*$ be a subgroup of index $m \mid p-1$.

Theorem 4.2. (See Fig. 3.) *The following are all cyclic Schur rings of dimension* $d=3$:

(1) $D_1=K$, $D_2=H \setminus K$, $D_3=G \setminus H$ *where* $K \subsetneqq H \subsetneqq G$.
(2) $D_1=H$, $D_2=g^{\Delta_2}H$, $D_3=g^{t\Delta_2}H$ *where* $[G:H]=p$ *which is an odd prime.*

Remark. Theorem 4.2 can also be considered as a consequence of Lemma 1.4. Actually, such a result can be traced back to the work of Schur [10].

Theorem 4.3. (See Fig. 4.) *The following are all cyclic Schur rings of dimension* $d=4$:

(1) $D_1=L$, $D_2=K \setminus L$, $D_3=H \setminus K$, $D_4=G \setminus H$ *where* $L \subsetneqq K \subsetneqq H \subsetneqq G$.
(2) $D_1=H \cap K$, $D_2=K \setminus H$, $D_3=H \setminus K$, $D_4=G \setminus (H \cup K)$ *where* $H \not\subset K$, $K \not\subset H$ *and* $HK=G$.
(3) $D_1=K$, $D_2=h^{\Delta_2}K$, $D_3=h^{t\Delta_2}K$, $D_4=G \setminus H$ *where* $[H:K]=p$ *where* p *is an odd prime.*
(4) $D_1=K$, $D_2=H \setminus K$, $D_3=g^{\Delta_2}H$, $D_4=g^{t\Delta_2}H$ *where* $[H:K]=p$ *where* p *is an odd prime.*

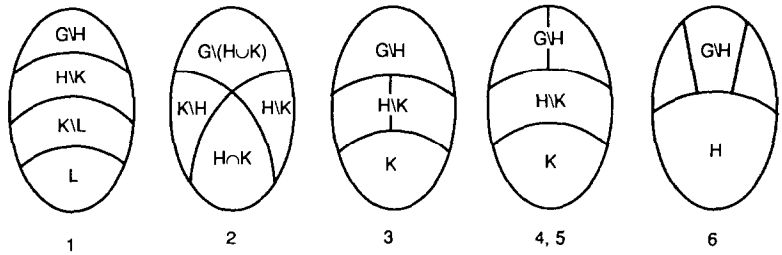

Fig. 4.

(5) $D_1 = K$, $D_2 = g^2K$ $(= H \setminus K)$, $D_3 = gK$, $D_4 = g^3K$ *where* $[G:H] = [H:K] = 2$.

(6) $D_1 = H$, $D_2 = g^{\Delta_3}H$, $D_3 = g^{t\Delta_3}H$, $D_4 = g^{t^2\Delta_3}H$ *where* $[G:H] = p$ *where* p *is an odd prime and* $p \equiv 1 \bmod 3$.

Remark. The same result can be found in [8] with a different proof.

By decomposing rational Schur rings of dimension $d = 2, 3$ and 4, all nonrational Schur rings of dimension $d = 5$ can also be constructed. Using the method described in the remark of Theorem 4.1, we can determine nearly all cases except the decomposition of Example 5 in Section 2 where $D_1 = H \cap K$, $D_2 = K \setminus H$, $D_3 = H \setminus K$, $D_4 = G \setminus (H \cup K)$ with $H \not\subset K$, $K \not\subset H$ and $HK = G$. (See Fig. 5.)

In order to obtain a nonrational Schur ring S of dimension $d = 5$, we have to break D_4 into two S-principal subsets, say D and $D_4 \setminus D = D^{(t)}$ for some integer t relatively prime to $|G|$. By a detailed investigation, it can be shown that, in this case, $|H| = p$ and $|K| = q$ must be primes. Moreover, a Schur ring exists if and only if $\Omega = \{t \in \mathbb{Z}_{pq}^* \mid D^{(t)} = D\}$ is a subgroup in $\mathbb{Z}_{pq}^*$ of index 2; $\{t' \in \mathbb{Z}_p^* \mid t' \equiv t \bmod p$ for some $t \in \Omega\} = \mathbb{Z}_p^*$ and $\{t'' \in \mathbb{Z}_q^* \mid t'' \equiv t \bmod q$ for some $t \in \Omega\} = \mathbb{Z}_q^*$.

Note added in proof. Concerning Section 3, we recently learned that results on Schur rings over cyclic p-groups also appeared in [4, 9]. However, our approach and methods are completely different from theirs.

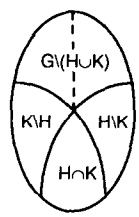

Fig. 5.

References

[1] E. Bannai and T. Ito, Algebraic Combinatorics I: Association Schemes (Benjamin/Cumming, Menlo Park, CA, 1984).
[2] P. Camion, Difference Sets in Elementary Abelian Groups (Presses de l'Université de Montréal, Montreal, 1979).
[3] B. Courteau and J. Wolfman, On triple-sum-sets and two or three weights codes, Discrete Math. 50 (1984) 179–191.
[4] J.J. Gol'fand, N.L. Najmark and R. Pöschel, The structure of S-rings over $\mathbb{Z}_{2^n}$, Preprint P-MATH-01/85, Institut für Mathematik, Berlin, 1985.
[5] S.L. Ma, Partial difference sets, Discrete Math. 52 (1984) 75–89.
[6] S.L. Ma, Polynomial addition sets and symmetric difference sets, in: D. Ray-Chandhuri, ed., Coding Theory and Design Theory, Part II, IMA Volumes in Mathematics and its Applications (Springer, Berlin, 1990) 273–279.
[7] S.L. Ma, On association schemes, Schur rings, strongly regular graphs and partial difference sets, Ars Combin. 27 (1989) 211–220.
[8] S.L. Ma, Schur rings and cyclic association schemes of class three, Graphs Combin. 5 (1989) 355–361.
[9] R. Pöschel, Untersuchungen von S-ringen, insbesondere im Gruppenring von p-Gruppen, Math. Nachr. 60 (1974) 1–27.
[10] I. Schur, Sur Theorie der einfach transitiven Permutationsgruppen, Sitzungsber. Preuss. Akad. Wiss. Berlin, Phys.-Math. Kl. (1933) 598–623.
[11] W. Scott, Group Theory (Prentice Hall, Englewood Cliffs, NJ, 1964).
[12] T. Storer, Cyclotomy and Difference Sets (Markham, Chicago, 1967).
[13] O. Tamaschke, Schur-Ringe, BI-Hochschulskripten 735 a^* Bibliographisches Institut, Mannheim, 1970.
[14] H. Wielandt, Zur Theorie der einfach transitiven Permutationsgruppen II, Math. Z. 52 (1949) 384–393.
[15] H. Wielandt, Finite Permutation Groups (Academic Press, New York, 1964).